

TeleTrust-Informationstag

"Elektronische Signatur und Vertrauensdienste"

Berlin, 27.09.2023

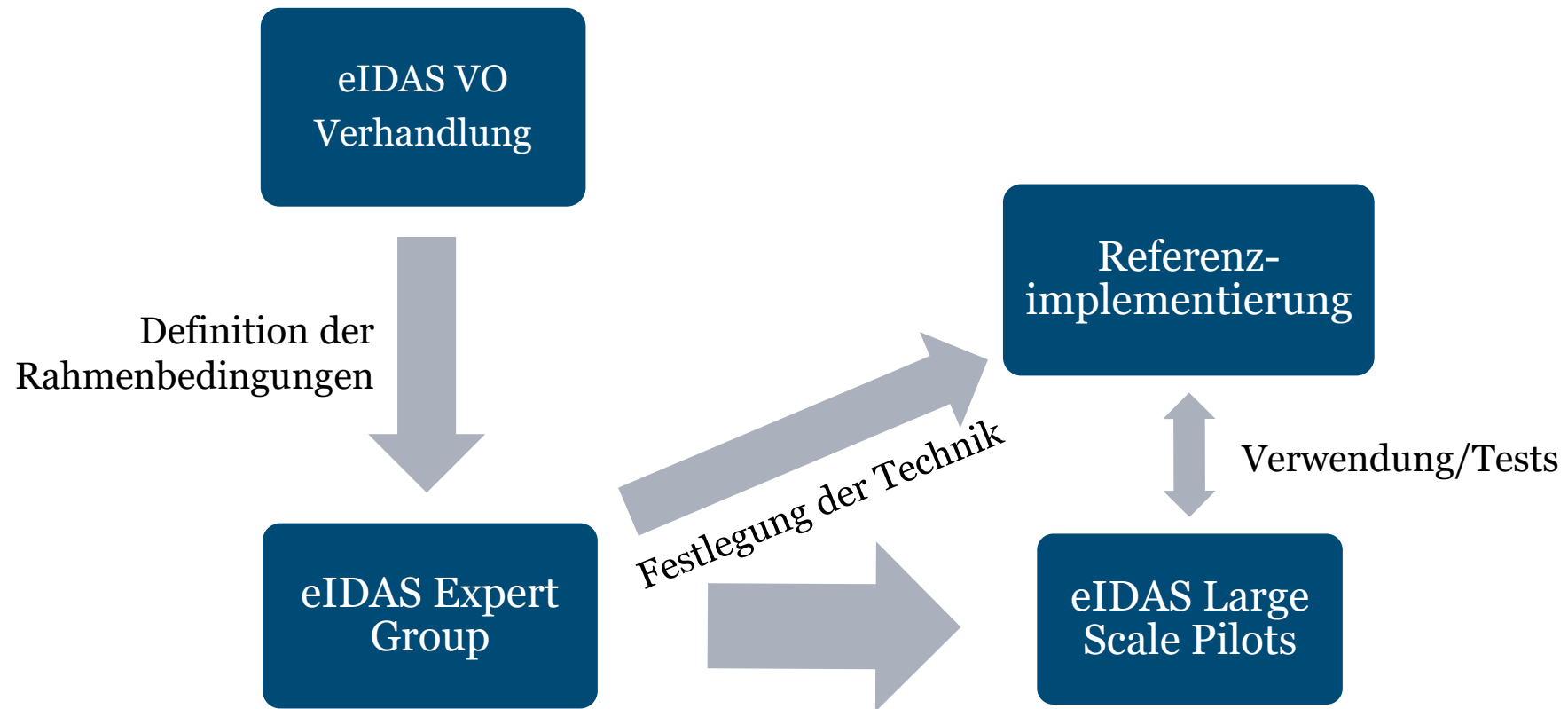
Neues zur deutschen Beteiligung an Expert Group, ARF und LSP

Dr. Felix Bleckmann,
Bundesamt für Sicherheit in der Informationstechnik

Inhalte der eIDAS Revision

- Turnusgemäße Überarbeitung der eIDAS Verordnung
- Kern ist die Schaffung eines Identitäten-Ökosystems mit der Wallet im Zentrum
- Zusatzfunktionen wie Übermittlung von Attributen und QES
- Bessere Anbindung der Privatwirtschaft
- Wechsel auf Harmonisierung in Form von Zertifizierung

Handlungsstränge im Kontext der eIDAS Revision

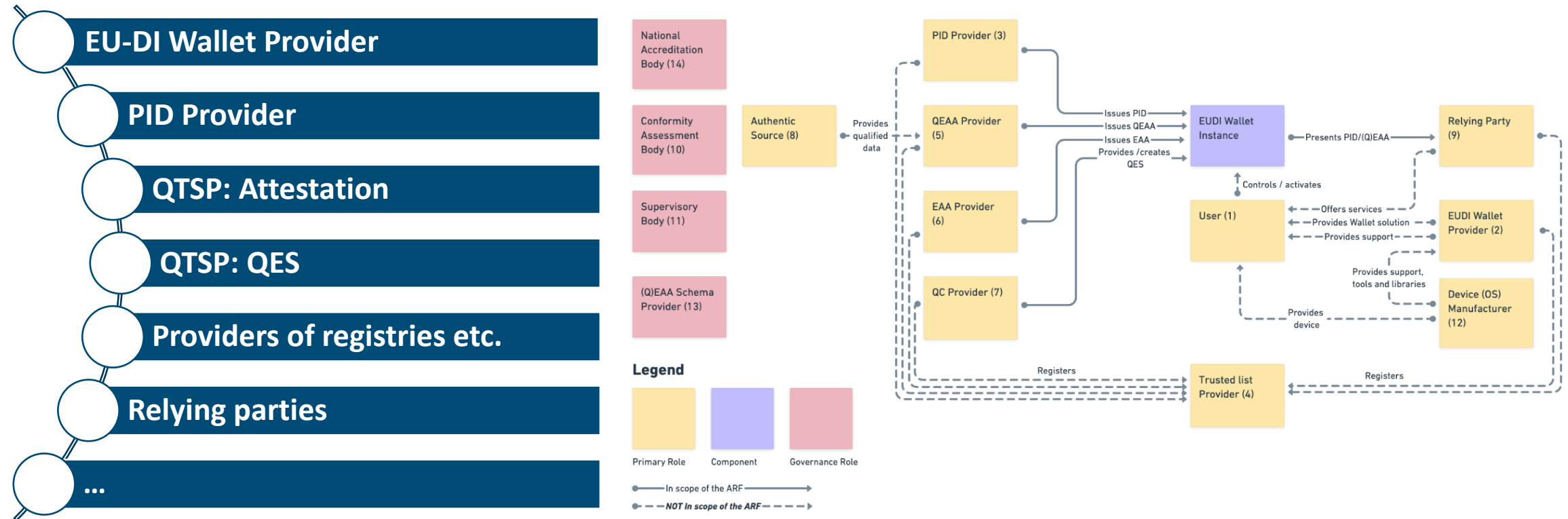


Neues von EG, ARF und LSP

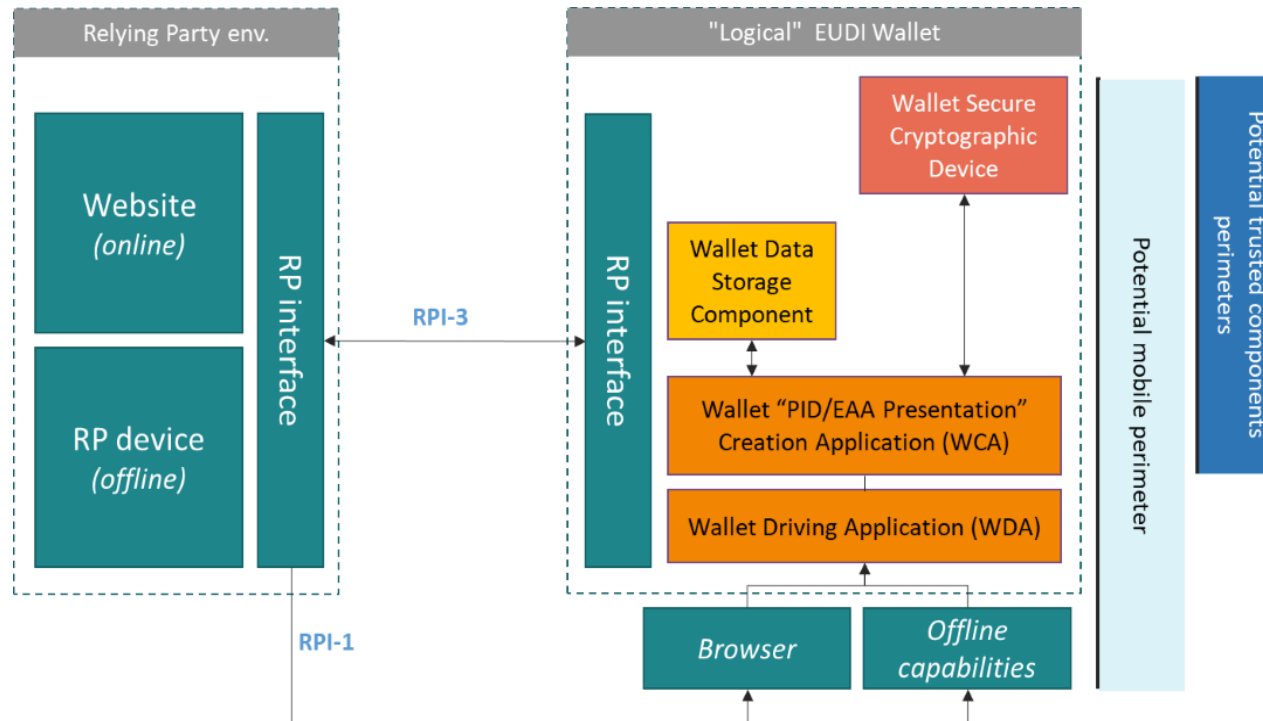
eIDAS Expert Group - ARF 1.1.0



Die Rollen im Ökosystem nach ARF 1.1.0



Grobe Architektur



Quelle: European Digital Identity Architecture and Reference Framework (April 2023)

WCA: Creates the (verifiable) presentation of PID/QEAA to be shared with the RP, based on the inputs received by the WDA

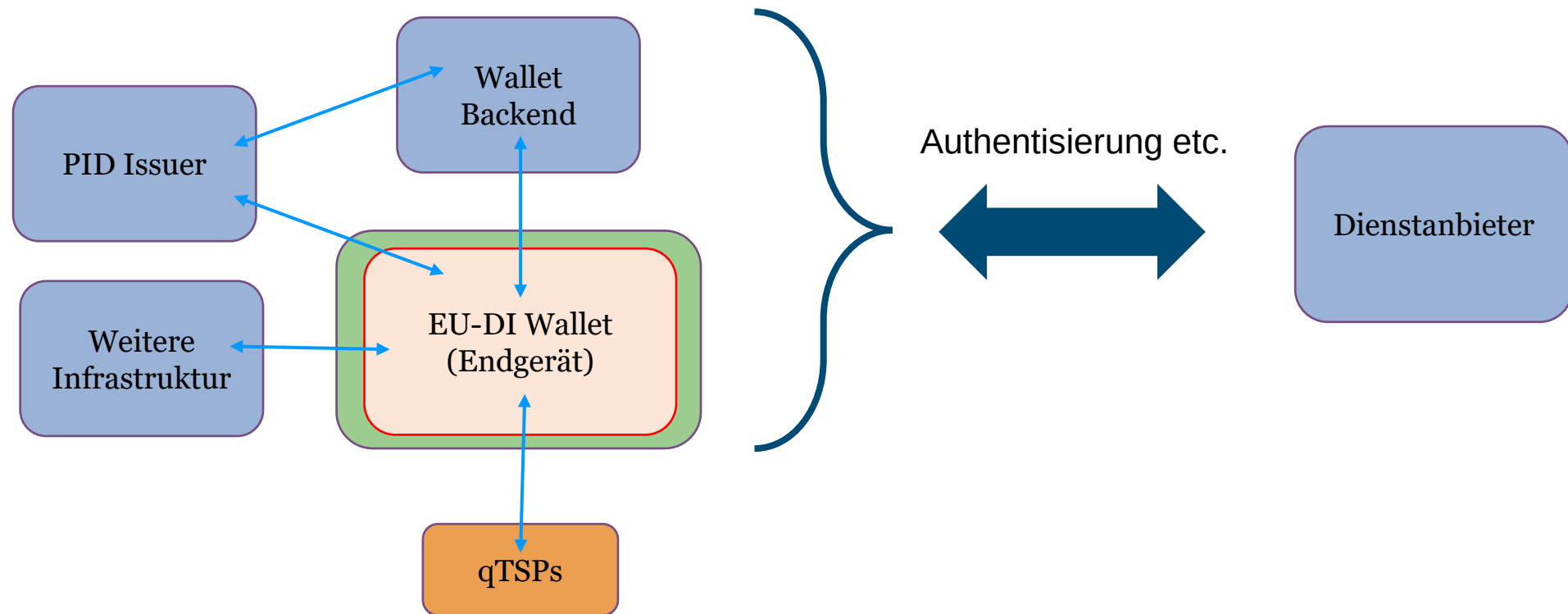
WDA: Provides the input to the WCA, such as:

- Which PID/EAA to combine based on user selection
- Which specific attributes to present (and which not to present) based on user selection

The UI (or part of it) is part the WDA

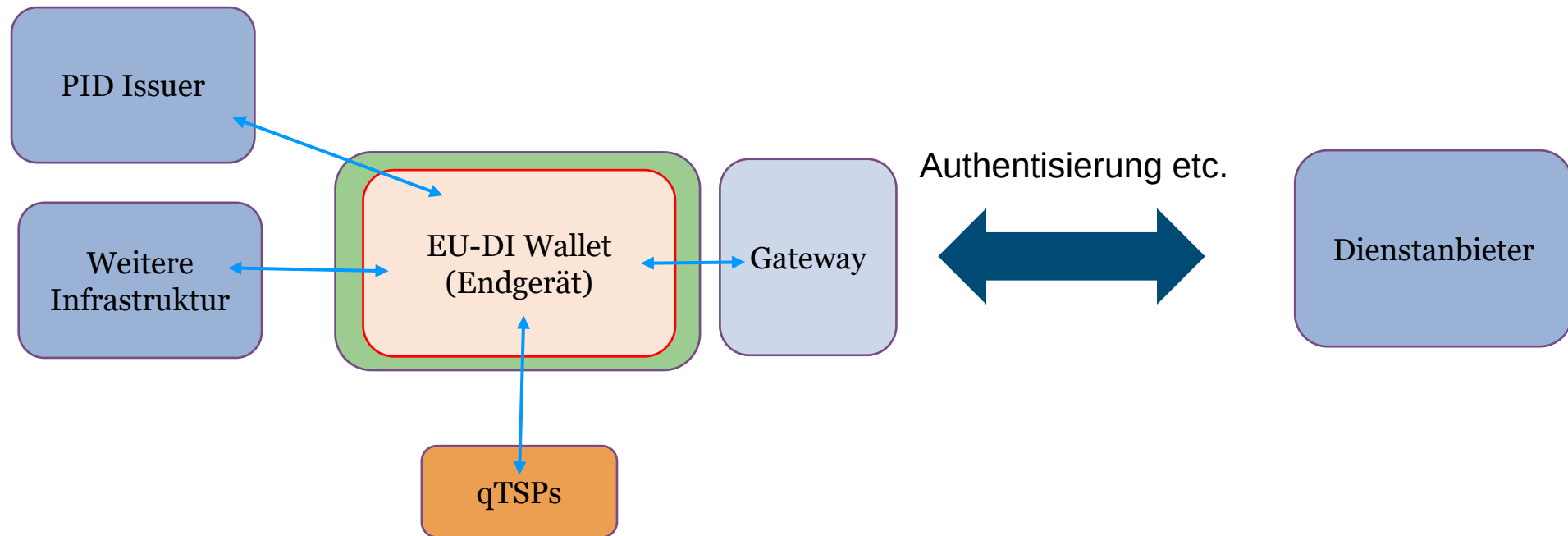
→ Weiterhin verschiedene Implementierungen denkbar

Zentraler Ansatz – Eine (vereinfachte) Skizze



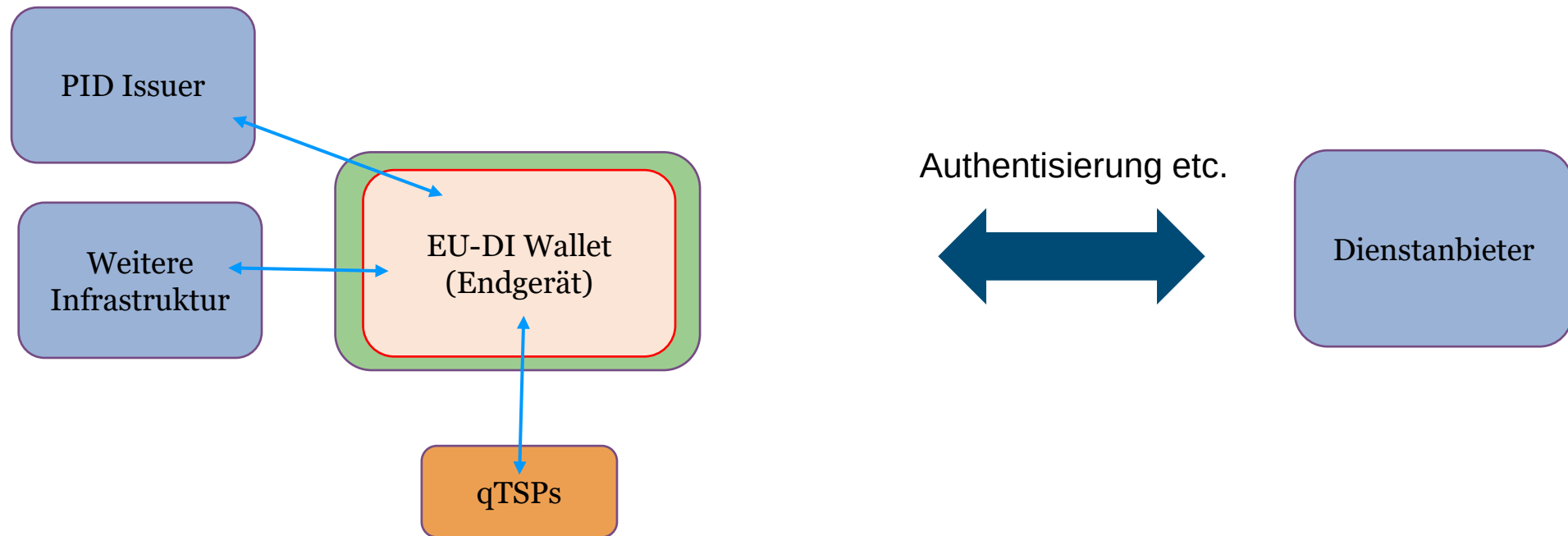
- Daten teilweise im Endgerät, teilweise im Backend (oder Register)
- Zusätzliche Daten können on-the-fly bezogen werden
- „Wallet“ bezeichnet das gesamte System aus Backend und App

Dezentraler Ansatz – Eine weiter (vereinfachte) Skizze



- Daten im Endgerät hinterlegt (oder auch in lokaler eID/Chipkarte)
- Zusätzliche Daten können on-the-fly bezogen werden
- Gateway verhält sich als „Wallet“ für Dienstanbieter

Dezentraler Ansatz – Eine weiter (vereinfachte) Skizze



- Daten im Endgerät hinterlegt (oder auch in lokaler eID/Chipkarte)
- Zusätzliche Daten können on-the-fly bezogen werden
- „Wallet“ hier nur auf Endgerät, weitere Infrastruktur von außen unsichtbar

Neues von EG, ARF und LSP

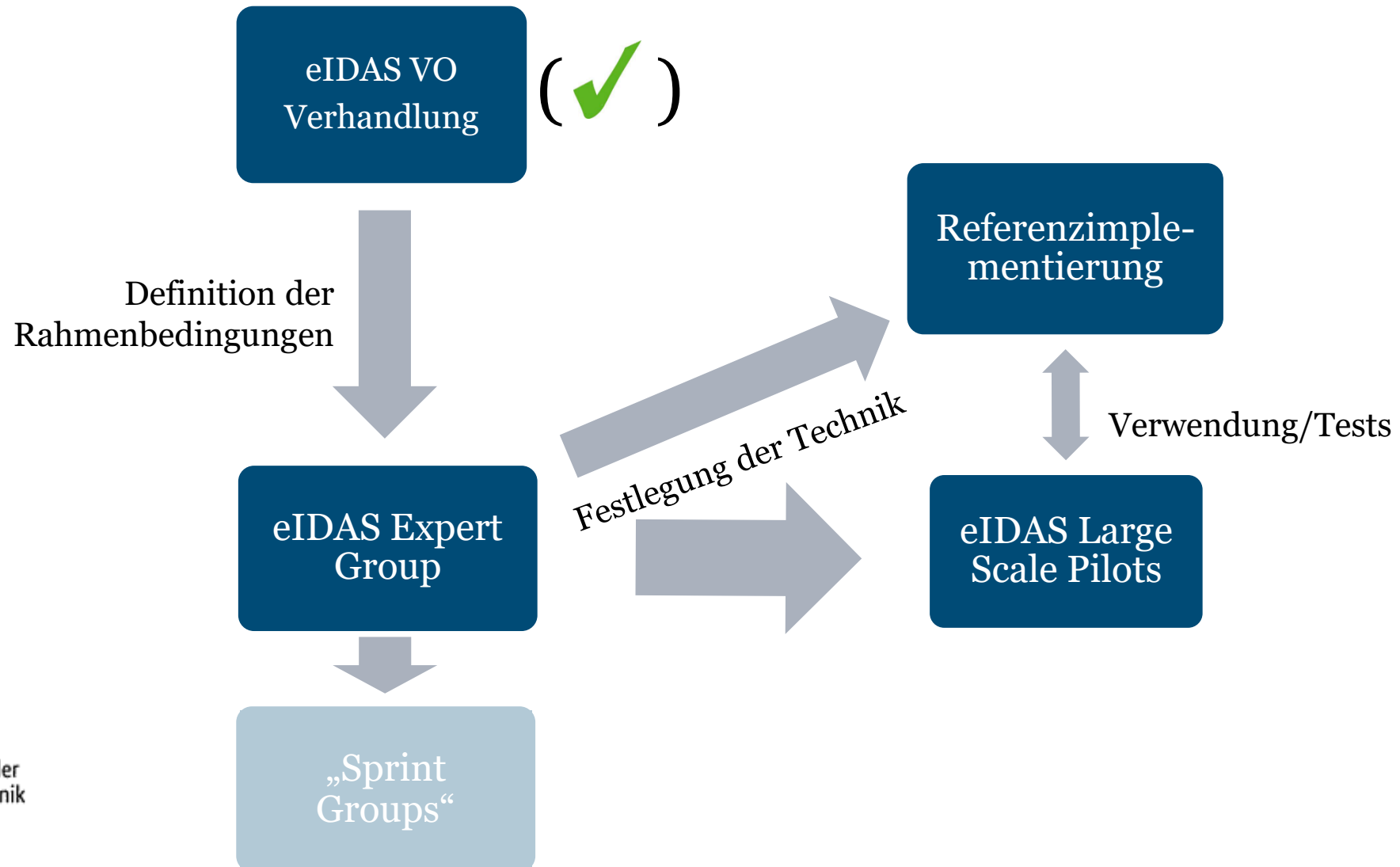
eIDAS Expert Group - Sprints



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Handlungsstränge im Kontext der eIDAS Revision



Sprint Status - Überblick

Sprint	Status	From	To	Epics	Phase I: Backlog refinement	Phase II: Implementation	Phase III: Review	Phase IV: Release	Published
Sprint #5	Implementation IN-PROGRESS	2023-08-31	2023-10-05	- EPIC-36-Risk analysis of the European Digital Identity Wallet usage - EPIC-27-Relying Party registration - EPIC-33-EUDI Wallet backup and restore - EPIC-34-Migrate to a different wallet solution - EPIC-35-PID Issuance service blueprint	S5. Phase I: Backlog refinement and planning	S5. Phase II: Implementation			
Sprint #4	Reviewing IN-PROGRESS DELAYED	2023-09-14	2023-10-05	- EPIC-10-Issuing a (Q)EAA to the EUDI Wallet - EPIC-11-Pseudonym attestation - EPIC-16-Signing documents with EUDI Wallet - EPIC-23-User requesting for a digital identity	S4. Phase I: Backlog refinement and planning	S4. Phase II: Implementation	S4. Phase III: Review	S4. Phase IV: Release	
Sprint #3	Release IN-PROGRESS DELAYED	2023-04-27	(ETA TBC)	- EPIC-06-Relying Party authentication - EPIC-07-PID and mDL validity checks and revocation - EPIC-08-EUDI Wallet Design Guide – Design Solutions on Data Sharing scenarios	S3. Phase I: Backlog Refinement and Planning	S3. Phase II: Implementation	S3. Phase III: Review	S3. Phase IV: Release	
Sprint #2	CLOSED	2023-03-27	2023-06-21	- EPIC-03-EUDI Wallet rulebook for online identification and authentication use case - EPIC-04-EUDI Wallet rulebook for proximity use case of mobile Driving License (mDL) - EPIC-05-EUDI Wallet Design Guide	S2. Phase I: Backlog Refinement and Planning	S2. Phase II: Implementation	S2. Phase III: Review	S2. Phase IV: Release	
Sprint #1	CLOSED	2023-02-13	2023-04-20	- EPIC-01-Accessing Public and Private Online Services with EUDI Wallet - EPIC-02-Mobile Driving License with EUDI Wallet	S1. Phase I: Backlog Refinement and Planning	S1. Phase II: Implementation	S1. Phase III: Review	S1. Phase IV: Release	ARF v1.1.0

Sprint Status - Überblick

Sprint	Status	From	To	Epics	Phase I: Backlog refinement	Phase II: Implementation	Phase III: Review	Phase IV: Release	Published
Sprint #5	Implementation 	2023-08-31	2023-10-05	- EPIC-36-Risk analysis of the European Digital Identity Wallet usage - EPIC-27-Relying Party registration - EPIC-33-EUDI Wallet backup and restore - EPIC-34-Migrate to a different wallet solution - EPIC-35-PID Issuance service blueprint	S5. Phase I: Backlog refinement and planning	S5. Phase II: Implementation			
Sprint #4	Reviewing  	2023-09-14	2023-10-05	- EPIC-10-Issuing a (Q)EAA to the EUDI Wallet - EPIC-11-Pseudonym attestation - EPIC-16-Signing documents with EUDI Wallet - EPIC-23-User requesting for a digital identity	S4. Phase I: Backlog refinement and planning	S4. Phase II: Implementation	S4. Phase III: Review	S4. Phase IV: Release	
Sprint #3	Release  	2023-04-27	(ETA TBC)	- EPIC-06-Relying Party authentication - EPIC-07-PID and mDL validity checks and revocation - EPIC-08-EUDI Wallet Design Guide – Design Solutions on Data Sharing scenarios	S3. Phase I: Backlog Refinement and Planning	S3. Phase II: Implementation	S3. Phase III: Review	S3. Phase IV: Release	
Sprint #2	 	2023-03-27	2023-06-21	- EPIC-03-EUDI Wallet rulebook for online identification and authentication use case - EPIC-04-EUDI Wallet rulebook for proximity use case of mobile Driving License (mDL) - EPIC-05-EUDI Wallet Design Guide	S2. Phase I: Backlog Refinement and Planning	S2. Phase II: Implementation	S2. Phase III: Review	S2. Phase IV: Release	
Sprint #1	 	2023-02-13	2023-04-20	- EPIC-01-Accessing Public and Private Online Services with EUDI Wallet - EPIC-02-Mobile Driving License with EUDI Wallet	S1. Phase I: Backlog Refinement and Planning	S1. Phase II: Implementation	S1. Phase III: Review	S1. Phase IV: Release	ARF v1.1.0

Veröffentlichung offen



Sprint Status - Details

- Als Version 1.2.0 „adopted“ aber noch nicht veröffentlicht wegen dem laufenden TRILOG sind u.a.:
 - Detailänderungen zum Wallet Instance Lifecycle
 - Erste Punkte zum Trust Model
 - PID Attribute
- In Bearbeitung sind u.a.:
 - Relying Party Registrierung, Authentisierung und Autorisierung
 - Ausgabe von PIDs und QEAs
 - ...

→ Weiterhin offen ist z.B. wie Vertrauensniveau hoch einheitlich sichergestellt wird!

Neues von EG, ARF und LSP

eIDAS Expert Group - Zertifizierung



Bundesamt
für Sicherheit in der
Informationstechnik

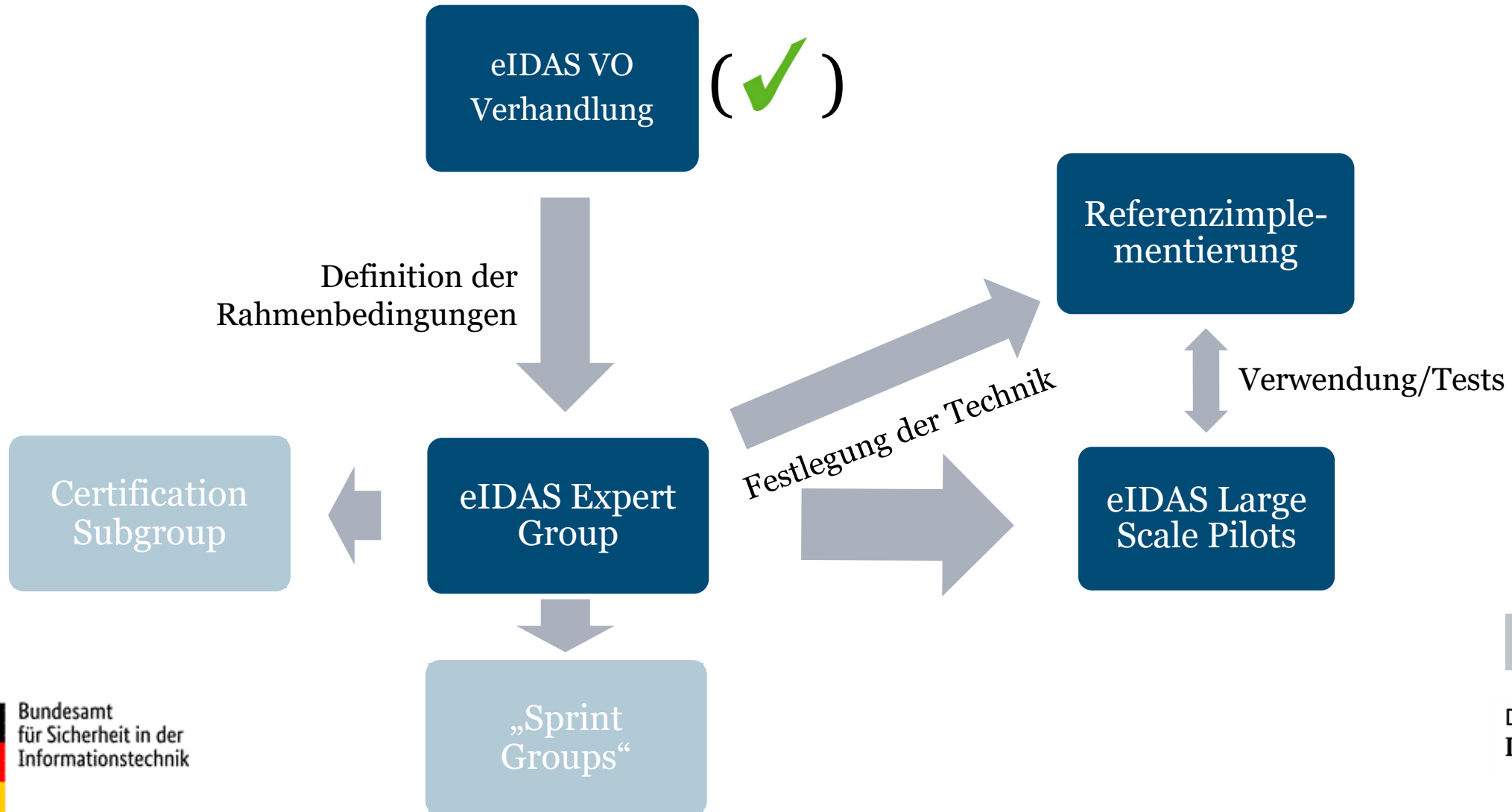
Deutschland
Digital•Sicher•BSI•

Was sagt die VO?

- Zertifizierung anstelle von Notifizierung
- Zertifizierung soll Erfüllung von Bestimmungen aus Artikel 6a sicherstellen
- Das bedeutet u.a.:
 - Funktionen/Interfaces werden bereitgestellt
 - QES werden ermöglicht
 - Datenschutzanforderungen werden erfüllt
 - Vertrauensniveau hoch wird erfüllt
 - ...

→ Zertifizierungsschemata müssen noch entwickelt werden

Handlungsstränge im Kontext der eIDAS Revision



Certification Subgroup

- Besteht aus Zertifizierern und eID Experten
- Fokus auf „Secure Components“
 - SEs, HSMs, etc.
- Muss Lösung finden:
 - für alle Designoptionen
 - für eine Übergangszeit bis der CSA fertig ist
 - ...

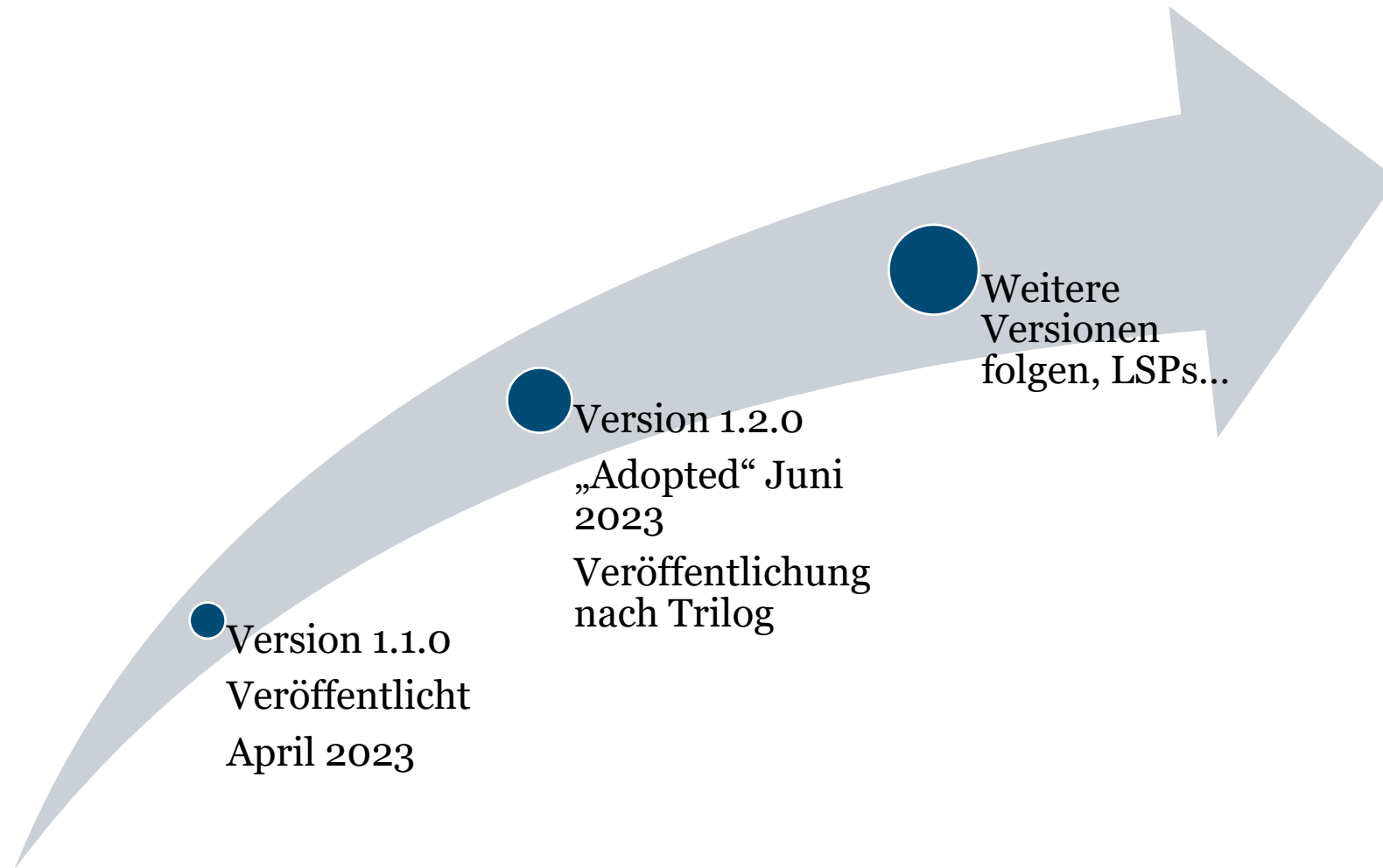


Bild: Arthimedes / shutterstock.com

Neues von EG, ARF und LSP

Zeitplan

Ausblick



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Felix Bleckmann
Referat DI 12

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Deutschland
Digital•Sicher•BSI

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.



Bundesamt
für Sicherheit in der
Informationstechnik